"Despite My Security Settings…": Online Behaviour and Perceptions of White-Collar Crime

by

Katherine B. Rose

A thesis submitted to the Psychology Program in partial fulfillment of the requirements for the degree of Bachelor of Arts (Honours), Division of Social Sciences

Department of Psychology

Grenfell Campus

Memorial University of Newfoundland

April 2014

Approval

The undersigned recommend the acceptance of the thesis entitled

"Despite My Security Settings…": Online Behaviour and Perceptions of White-Collar Crime

Submitted by Katherine B. Rose

in partial fulfillment of the requirements for the degree of

Bachelor of Arts (Honours)

_____

Kelly Warren
Thesis Supervisor

_____

Kelly Brown
Second Reader

Grenfell Campus

Memorial University of Newfoundland

April 2014

Acknowledgements

It goes without saying that I would have not been able to complete this project to the best of my ability without the unwavering motivation and assistance of the whole Psychology Department at Grenfell Campus. I would like to thank the Psychology Faculty for their encouragement throughout the process of this Honours thesis. Each individual member went beyond their role as an educator to see me succeed in the Psychology program. I would like to thank Kelly Brown, who as my second reader took the time to read such a magnitude of text. Her patience in the final weeks of my project cannot go without acknowledgement. I must recognize Dr. Peter Stewart and Nadine Lindstone, who generously took time from their hectic schedules to answer my questions regarding statistics and formatting. In particular, I thank Peter Stewart for correcting my pronunciation of a chi square after all these years. I would also like to extend special gratitude to Dr. Jennifer Buckle for demonstrating support, encouragement and guidance throughout the final months of this project. Her open door policy was enormously helpful for every question, concern or update I had.

Lastly, I cannot thank Dr. Kelly Warren enough for her persistence in this project. Kelly Warren's passion for research was contagious, and thanks to her constant energy and never-ending ideas, I had an exceptionally exciting time conducting this study. When obstacles arose, Kelly Warren continuously adapted her schedule to my (constant) late-night edits and e-mails. I am indebted to her for the care she demonstrated to both the project and I.

Table of Contents

List of Figures

List of Tables

List of Appendices

Abstract

Previous research suggests a discrepancy between perceptions of online security and the level of privacy actually achieved. For example, the information made publically available on Facebook profiles can be used to answer popular security questions. This poses a risk for white-collar crime, whereby someone in a position of power manipulates others for financial gain. Examining whether individuals recognize the risk for white-collar crime is therefore an important step towards internet security. Active Facebook users (n = 501, M_{age} = 26.12 years) completed an online survey assessing online behaviour. Approximately half of participants had an experience where their privacy was compromised online. Despite these experiences, white-collar crimes were perceived as less serious than other online threats and participants failed to recognize the risk of providing information online. Education about safe online practices may be needed to raise awareness and to reduce the risk for online crime due to online disclosure.

"Despite My Security Settings…": Online Behaviour and Perceptions of White-Collar Crime

White-collar crime, better known as corporate crime, has been redefined over the years (Shapiro,1980; Simpson, 2013). Its definition has been a controversial issue among researchers (Helmkamp et al., 1996; Simpson, 2013). It was originally classified as the sophisticated crime within a corporate business by Edwin Sutherland in 1939 (Sutherland, 1940; Simpson, 2013). White-collar criminals were believed to be people of high socioeconomic status and power within corporations (Abel, 1945; Sutherland, 1940; 1945). However, white-collar crime can extend beyond the corporate offices. Arguably, white-collar crime can be classified today as crimes whereby those in positions of power deceive others for financial gain ("White-Collar Crime," n.d.). Such a definition encompasses the various forms of white-collar crimes and the means by which it may occur. The foundation for these crimes is in the abuse of trust and in the manipulation of others (Shapiro, 1990).

Hidden behind a computer screen, a white-collar criminal need only be in a position of power relative to his/her victim to commit the crime, and not necessarily a corporate powerhouse. Given the ease of access to personal information online, white-collar crimes can be easier to commit. While it is true that there are online security measures to protect against threats, there are loopholes. Specifically, the information made available on Facebook may be used to answer the security questions we use to protect our online information (e.g., online banking accounts). Thus, it is important to assess perceptions of white collar crime on the internet because despite security settings,

white-collar criminals can access crucial personal information. As online behaviours evolve, awareness and practice of online security must also advance.

Perceptions Versus the Reality of White-collar Crime

White-collar crime poses both a significant social and financial threat to victims (Abel, 2008). Fraud costs Canadians an estimated 10 billion dollars annually, besides the emotional devastation of its victims ("Fraud costs Canadians $10B annually: RNC," 2010). Victims may also feel guilty, embarrassed, frustrated and angry that their trust was abused and they may lose faith in powerful people (Sutherland, 1940). The exploitation of trust may deter victims from trusting ever again: a lifelong social consequence. For this reason, forms of white-collar crime, including fraud and identity theft are now on the radar of the FBI and the Royal Canadian Mounted Police ("Corporate Crime," 2012; "Fraud costs Canadians," 2010). For example, the FBI lists tips for online security to warn the public about the risks of sharing too much personal information, and falling for scams online (http://www.fbi.gov/about-us/investigate/white_collar, n.d.).

Despite the severity of its consequences, white-collar crime is perceived as less serious than other forms of crime (Holtfreter, Skyle, Bratton & Gertz, 2008; Rosenmerkel, 2001; Rossi, Bose & Berk, 1974). For example, when Rosenmerkel (2001) asked participants to rate various crimes in seriousness, wrongfulness and harmfulness, white-collar crime was rated as being less serious, wrong and harmful than violent crimes. Similarly, Rossi et al. (1974) found when participants were presented with a list of 140 crimes white-collar crimes were ranked lower in perceived seriousness than most of the other crimes listed. The majority of participants believed that violent

offenders, as opposed to white-collar offenders, would and should receive harsher punishments than their white collar counterparts (Holtfreter et al., 2008). It has been suggested that white-collar crime is seen as less serious than other forms of crimes because with the lack of direct physical contact, it is deemed victimless (Rosenmerkel, 2001).

To date, no studies have assessed perceptions of white-collar crime on the internet. Online fraud, identity theft and Ponzi schemes are just a few of the threats online users face. To defend or guard against such crimes, internet users use security measures such as security questions to protect their personal information. Yet, research to date has not assessed the perception of such crimes in terms of frequency for potential victimization.

The Role and Risk of Security Questions

Security questions, also known as challenge or personal verification questions, are used to confirm a user's identity when he/she has forgotten, or needs to change, a password (Just, 2004; Rabkin, 2008). For example, security questions are used for online banking, e-mail and Facebook accounts. Users may choose from a pool of security questions and create an answer that can confirm their identity. These questions are designed to trigger personal long term memories, thus the answers need not be memorized (Rabkin, 2008).

There are basic characteristics that make a personal verification question usable. First, the answer to the question must be simple and easy to remember (Rosen, 2007; Scoville, 2010). If the security question does not quickly trigger a memory, the individual will struggle to recall the answer to the question (Just, 2004; Rabkin, 2008). A

vague security question can pose a problem for users because answers are wide-ranging, and will not trigger the memory of the user (Just, 2004; Rabkin, 2008). A question such as "What was your dream job as a child?" poses a problem because people may have dreamed of a number of jobs throughout their childhood (e.g., doctor, nurse, firefighter, veterinarian, chef, teacher). Second, a usable security question should allow for a variety of answers among all users of that online program so that not many people share the same security answers (Rosen, 2007; Scoville, 2010). An inapplicable security question, or one that is irrelevant to the personal lives of consumers, means that it is just too specific to be used by many diverse people (Just, 2004; Rabkin, 2008). For example, asking security questions about dogs is inapplicable because not everyone owns a dog; questions should be generalizable to users of online security. Third, a security question must also be definitive and stable so that the answer does not change over time (Just, 2004; Rosen, 2007; Scoville, 2010). Last, the answer to the security question should be difficult to guess or determine by studying personal details about the individual (Just 2004; Rabkin, 2008).

Websites dedicated to online security suggest there is no "good" security question (Rosen, 2007; Scoville, 2010). There is a trade-off between the usability of a security question and the security of the question (Just, 2004). For example, the more complicated the answer to the security question is, the more difficult it is to remember and recall quickly. However, a simple answer may pose a security risk as it could be easy to search for this information. Many security questions are undeniably attackable in that the answers can be obtained by those other than the user (Rabkin, 2008). Common

topics among security questions in major online banks include family names and favourite things (Rabkin, 2008).

Rabkin (2008) coined the term, “automatically attackable” to refer to security questions that could be answered using information collected from social networking sites such as Facebook (p. 5). Rabkin (2008) found that 12% of the online bank security questions examined were automatically attackable. A compromised Facebook account could indeed be problematic because someone can act as the puppeteer behind another’s Facebook account, while remaining undetected. This means not only does the person have access to someone’s personal settings, Facebook friends, photographs and statuses, but he/she can also view and change the personal details in the account. Yet, the risk is not excluded to having someone else behind the Facebook account (Rabkin, 2008). The amount of public information available online through social media sites could very well pose a security threat. Accessible information on a Facebook profile could help others break into the Facebook account or other online accounts by providing answers to security questions.

Common security questions can be broken down into 10 categories based on themes in the questions and answers. The largest categories are family related, (e.g., What is your mother’s maiden name?), location related (e.g., In what city or town was your first job?), history related questions (e.g., What is the first car you ever owned) and education related questions (e.g., What is the last name of your first grade teacher?). Other categories include: animal related (e.g.,. What is the name of your first pet?); personal interest related (e.g., Who was your childhood hero?); personal characteristics (e.g., what is the color of your eyes?); work related (e.g., What is the name of the

company of your first job?); life event related (e.g., What month and day is your anniversary?); and personal contact information (e.g., What is your address?) questions. It is important to organize the type of security questions that are commonly used because the information provided on Facebook may be similarly categorized. As Rabkin (2008) noted, information about family members and favourite things are not hard to discover on a social media profile.

The Risk of Facebook

Social media sites, such as Facebook, are potentially putting users at risk for online white-collar crime. Privacy and security concerns are rising with the increasing popularity of Facebook (Lemieux, 2012). Millions of Facebook users share personal information on their profiles for Facebook friends and strangers to see (Houghton & Joinson, 2010). As of March 2013, Facebook reached 1.11 billion users, with 665 million users logging on per day (The Associated Press, 2013). Of its active users, not everyone has the highest privacy settings necessary to protect their personal details, details that can be used to answer security questions. Is it really that easy? Yes it is. In September of 2012, a man named Dave had individuals recruited for a psychic reading. Dave astounded participants with his ability to know of their hidden tattoos, house for sale, motorcycle color, and even spending habits (Guillaume, 2012). Before he was done however, the black screen behind Dave dropped to reveal that all of the personal information had been obtained in live-time from details available on the internet. The participants were shown a screen reading, "Your entire life is online. It might be used against you" (Guillaume, 2012). More recently, a Canadian woman learned that posting about an absence away from home could have serious consequences; she was robbed of

$20,000 worth of goods while she was out of town and blamed her Facebook post for alerting robbers to the empty home (Ramachandran, 2013).

Personal information is bountiful on social media profiles (Christofides, Muise & Desmarais, 2009; Fogel & Nehmad, 2009; Lemieux, 2012; Sophos, 2009). Facebook prompts users to add photographs, check in at various locations, list family members, and to create a timeline of life events. With details at risk, users would benefit from hyper vigilant behaviours in protecting their privacy. However, Facebook users sometimes accept a stranger's friend request and consequently give up personal information to the individual behind the account (Lemieux, 2012; Sophos, 2009). In an assessment of this, Lemieux created a gender neutral Facebook account and friend requested 450 graduate students on campus. The profile of Jamie Marple was made to look like an active Facebook user through the correspondence of accomplices (Lemieux, 2012). A total of 325 students friended Jamie Marple without ever meeting or knowing who he/she was.

Similarly, in 2007, Sophos online security company conducted a study using "Freddi Staur", a Facebook account with a profile picture of a toy frog (Sophos, 2009). "Freddi" friend requested 200 Facebook users and was accepted by 87 (Sophos, 2009). A total of 72% of respondents provided an e-mail address, 84% gave their full birthday, 87% listed their education or workplace, 78% gave their current address/location, and 23% listed their current phone number (Sophos, 2009). Additional sensitive information was made available such as resumes, family names and personal details (Sophos, 2009). It is this information that when made available to others, can be used to answer security questions.

More recently, Christofides et al. (2009) examined the Facebook profiles of 343 students at an undergraduate institution. They found that 85% of participants gave their e-mail address, 85% shared their hometown, and 72% shared their school and program. Almost all participants (97%) were members of a network, or a group, on Facebook. In a Facebook group, such as those created for clubs, similar interests, or graduating classes, members can be viewed by everyone else in the group. For example, the popular Facebook game, Candy Crush Saga, has brought in over 50 million monthly players (https://developers.facebook.com/docs/showcase/candycrushsaga/, n.d.). As part of the game, players may ask Facebook friends for assistance to improve their achievements in the game. Consequently, Facebook groups have emerged where strangers interact and help each other through the levels of Candy Crush. As of April 2014, one such group held 38,607 members ("Candy Crush Saga All Help," n.d.). Being part of such a group offers the profile to 38,606 people (Christofides et al., 2009). One does not have to accept someone as a Facebook friend to view information on his/her profile. Individuals who are not Facebook friends may be able to access personal details if the privacy settings of the account make it available to public viewers. Group members may not be aware of privacy settings within the group, or may not be aware of what they are revealing online.

Learning how to manipulate Facebook to gain power over others is not as difficult as one may think. Websites which describe how to hack into the Facebook accounts of others are easily accessible via the internet (Praveen, 2012). Such websites provide instructions on how to determine answers to security questions using social media sites and search engines (Praveen, 2012). With opportunity and effort, one could certainly

gain access to a person's Facebook account and either find answers to security questions from information viewable to the public or from inside the account. By being inside the Facebook profile, perpetrators can obtain extensive personal information. They may also take advantage of having somebody else's identity. One risk for deception for financial gain is family members or friends being asked for money. Individuals could also manipulate Facebook to commit white-collar crime by gaining access to other personal accounts, such as e-mail accounts or online banking through the information provided by Facebook. For example, online bank accounts ask for personal verification before allowing access to banking information.

Facebook allows users to access personal information about even their closest friends (Chaulk & Jones, 2011). Chaulk and Jones examined how obsessive relational intrusion can be expressed in online contact and behaviour. Of the 230 individuals surveyed, 75% claimed to have used Facebook profiles to obtain information about an acquaintance, while 70% did so for a close friend and 52% did so for an ex-partner (Chaulk & Jones, 2011). Similarly, Alexander (2011) noted that Facebook users show increased cyber monitoring for their romantic partners. This means that users watch the online behaviours of their partners by observing the adding of Facebook friends, wall posts and photos (Alexander, 2011). Facebook is clearly being used as a "surveillance tool" (Alexander, 2011, p. 24). However, only 41% of participants in Chaulk and Jones believed that acquaintances had used their profile to determine information about them. While people are invading the privacy of others, not everyone believes they are victims of the same surveillance behaviours.

The Illusion of Control

In Facebook's Statement of Rights and Responsibilities, users must agree to "[not] do anything else that might jeopardize the security of [their] account" ("Statement of Rights and Responsibilities," 2013). Yet, merely including personal details on a profile poses a threat to security. Users must agree to the Statement of Rights and Responsibilities (SRR), which states the relationship Facebook has with its users and others, in order to use Facebook ("Statement of Rights and Responsibilities," 2013). In the same way, Facebook's Data Use Policy educates users on how their information may or may not be used (Data Use Policy, 2013). It contains details regarding the use of user's information by Facebook and third parties (Data Use Policy, 2013). For example, all Facebook pages are public, thus any information posted on a page becomes available to anyone and everyone (Data Use Policy, 2013). Furthermore, if a user decides to delete his/her account, it is not deleted immediately; there is a time lapse before the information is removed (Data Use Policy, 2013). Information can be stored for up to 90 days after an account is deleted (Data Use Policy, 2013). In the Data Use Policy (2013), Facebook warns its users that even if a profile is privatized so that it cannot be searched by others it is still accessible. For example, if someone has the username of the profile, known as the User ID or User URL, the username can be added to Facebook's URL and it will open the public profile of the target. Using a user's Facebook username is one of the steps described in hacking into a Facebook account (Praveen, 2012).

Do Facebook's SRR and Data Use Policies demonstrate good online security? The argument appears to be that they do not. Facebook does offer its users control over their privacy, but there are limitations in how much privacy control users have

(Christofides, Muise, & Desmarais, 2012). For example, profile pictures are always publically available (Data Use Policy, 2013). Furthermore, users may not be aware of where to find privacy settings as they are not easily labeled to suit the needs of all users (i.e., young and old) (Christofides et al., 2012). Facebook's Data Use Policy describes how to check what information is available about the person but it is deep within the lengthy script and not obvious to the reader. This raises a concern that users may not fully read nor understand the information in Facebook's policies.

The illusion of control can be dangerous to Facebook users' privacy. Simply put, not everyone is aware of the risks. To demonstrate, Stutzman, Capra and Thompson (2011) surveyed university Facebook users on privacy attitudes, use of privacy settings, the intake and understanding of Facebook's privacy policy and information disclosed on Facebook. A total of 87% of participants changed and customized their Facebook privacy settings from the default settings, demonstrating their use of control when available (Stutzman et al., 2011). However, the study revealed that *only* the privacy concern of information leakage (out of identity theft, hackers, blackmail and cyber-stalking) increased the use of such privacy protecting behaviours (Stutzman et al., 2011). This suggests that people may not perceive a risk for other considerable online threats such as white-collar crime. The fact that the perception of risk fluctuates amongst users, when the risk is always present, is concerning. Only those who held a great concern for privacy read most or all of Facebook's privacy policy instead of scanning it and disclosed less on Facebook (Stuzman et al., 2011). Customization of who could view information on the profile doubled the likelihood that users would disclose a lot of personal information online (Stuzman et al., 2011). This suggests that perceptions of control lead

to more disclosure because Facebook users feel safer posting particular information. Yet if this perception is an illusion, there is still a risk in posting personal details. In reality, the risks exist for those who are concerned and those who are not. Consumers of Facebook have very little control according to the Data Use Policy and SRR. It is crucial to educate users who are unaware of Facebook's risks.

Why Do People Still Use Facebook?

The benefits of using Facebook seem to outweigh the risks for many users (Debatin, Lovejoy, Horn & Hughs, 2009). Users must provide substantial information to be found on Facebook, where they can participate in rewarding social interactions (Christofides et al., 2012). It may not be possible or advisable to discourage people from using Facebook. However, there may be other measures that can be taken to decrease security threats such as identity theft and/or fraud (Christofides et al., 2012). For example, there is a need to encourage Facebook users to be aware of, and to use strict privacy settings before negative interactions happen. In a study assessing adolescents' perceptions of Facebook privacy and bad experience, Christofides et al. found a significant positive relationship between having a bad experience on Facebook and knowledge of the privacy settings (Christofides et al., 2012). Thus, those who had a negative experience on Facebook were more likely to understand and use their privacy settings on Facebook (Christofides et al., 2012). Christofides et al. found that 26.7% of surveyed adolescents had experienced a specific negative experience on Facebook, such as bullying, unintended disclosure, and unwanted contact. Yet, they remained on Facebook.

The online experiences users have on Facebook clearly influence how people use the webpage. Those who have a bad experience on Facebook are more likely to practice safer online behaviours and to become more aware of privacy settings (Christofides et al., 2012). Furthermore, Facebook users are more likely to make protective changes to their Facebook account when they perceive a personal risk (Debatin et al., 2009). Likewise, Debatin et al. found that most users were aware of Facebook's privacy concerns and consequently restricted their profiles, but those who were not familiar with privacy risks did not limit their profiles. Ideally, Facebook users should not have to have a negative experience to become more hyper vigilant about their privacy. Including Facebook users in online research appears to be a great way to help them reassess their profiles and the type of information being made available (Nosko et al., 2012). The void in current literature needs to be filled to decrease the likelihood of negative Facebook experiences for its users.

Present Study

There is a need to explore perceptions of white-collar crime in online behaviour and to determine how Facebook users are at risk for white-collar crime such as identity theft and fraudulent scams. If Facebook users do not recognize the risk for white-collar crime in the information given on their Facebook profiles, they may not be aware of the measures they can take to protect their overall privacy. The current study examined how Facebook users perceive their online security on Facebook and explored the possibility for modern day white-collar crime. There are practical implications to the current study because businesses, such as Facebook, can learn whether changes are needed to protect the security of consumers. To assess these issues, a survey was developed to examine

perceptions of online behaviour and the risk for white-collar crime on Facebook. The survey assessed knowledge and understanding of privacy policies, risky behaviours, perceptions of white-collar crime compared to other online behaviours, and whether people identified the risk for online crime, including white-collar offenses, based on online disclosure. The survey also examined perceptions of a scenario depicting white-collar crime, including the best course of action, victim responsibility and the likelihood of the perpetrator being caught. Multiple hypotheses were developed related to the primary goals of the study.

Hypothesis #1: Facebook users would not recognize how particular information on a Facebook profile could be used to put someone at risk for a variety of online threats, including white-collar crime. Because Facebook users are revealing so much information, both to external viewers and to those whom they have as Facebook friends, this suggests that they do not recognize the relationship between the type of information made available and the risk it could pose (Chaulk & Jones, 2011; Christofides et al., 2009).

Hypothesis #2: Participants will have had an experience where either their Facebook account, or another online account, was compromised. Research into online security has demonstrated that obtaining personal information through Facebook is easy, and thus it is easy to break into online accounts using this information. For example, personal information can be used to answer the security questions to online accounts (Christofides, et al., 2009; Just, 2003; Lemieux, 2012; Rabin, 2008; Sophos, 2009).

Hypothesis #3:Facebook users would rank white-collar crime as a less serious threat than other online behaviours. Research into white-collar crime indicates that it is perceived as less serious than other forms of crime (Holtfreter et al., 2008; Rosenmerkel, 2001; Rossi et al., 1974). Furthermore, potential forms of white-collar crime such as identity theft, hacking and blackmail were not enough to change the privacy behaviours of young Facebook users (Stutzman et al., 2011)

Hypothesis #4: Active Facebook users would be engaging in online behaviours that decrease the privacy of themselves and others on Facebook, risking white collar crime. Previous research suggests that while Facebook users disclose information to enjoy social interactions, they are revealing details that can be used against them (Christofides et al., 2009; Debatin et al., 2009; Sophos, 2009; Lemieux, 2012). Furthermore, research suggests that Facebook users use the profiles of others to discover information about them, yet do not anticipate the same from others (Chaulk & Jones, 2011). This implies that Facebook users do not perceive a personal risk from others viewing their profile. Behaviours that could put Facebook users at risk include not only using profiles to obtain information, but accepting strangers as Facebook friends, not being aware of Facebook's privacy settings and underestimating the privacy of the account.

Method

Participants

A sample of 522 participants was originally obtained for the purposes of this study. However, only active Facebook users were included in data analysis. Seven participants did not declare themselves as active Facebook users and were therefore omitted. One participant was eliminated because the participant did not meet the minimum age requirement of 19 years. An additional 13 participants were not included in data analysis because they left a large majority of the survey incomplete (only answered first 5 questions). There was nothing in the data to indicate differences between those who did or did not complete the survey. Therefore, a total of 501 participants were used in this study, of which 329 were women, 82 were men, and 90 did not specify a gender. The mean age of participants ranged from 19-66 (M = 26.12 years, SD = 9.68).

Materials

For the purposes of this study, a survey was created using Survey Monkey. Before beginning the survey, participants were presented with an informed consent notice. The informed consent notice provided participants with information regarding the risks and benefits of the study, confidentiality, anonymity and their right to end the survey at any time. Names and contact information of the researchers were provided in case of questions or concerns. A copy of the informed consent notice is available in Appendix A.

The questionnaire assessed various online experiences and perceptions of online behaviours. First, participants were questioned about their perceptions and awareness of

the privacy of their own Facebook profile. These questions were answered either on a Likert scale or in a "yes/no" format. Second, participants were asked about their experiences where online privacy may or may not have been jeopardized. This included "yes/no" style questions, as well as open-ended questions where participants could detail their experiences. Third, participants were asked about personal behaviours that could jeopardize the security of other Facebook users, such as whether they had ever viewed an online profile to gain information, and if so, how often they had viewed such profiles. Fourth, participants ranked six threatening online behaviours based on perceived seriousness.

A scenario was used to assess perceptions of online behaviour. The scenario detailed the information made available on an individual's Facebook profile. Perceptions of what personal information posted on Facebook could create a risk for specific online threats were assessed. The final question of the survey provided participants with statistics detailing what 200 Facebook users provided on their profiles and the risk for white-collar crime by posting this information. Participants were asked how concerned they were that the details made public on their own accounts could put them at risk. Before viewing a debriefing notice, participants were given the option to consent to having their own Facebook profile privacy assessed by the researcher as an additional component of the study. A copy of the complete survey can be found in Appendix B.

Following the survey, a debriefing notice was used to inform participants of the details of the study, as well as to provide additional contact information for mental health services. A copy of the debriefing screen is included in Appendix C.

Only portions of the survey results were analyzed to assess the four hypotheses of the present study. Specifically, participants' indication of what pieces of information on a profile could put a user at risk for white-collar crime was assessed. Furthermore, participant' perceptions of their profile security, experiences of compromised privacy on Facebook and online, perceived concern for white-collar crime, and behaviours participants engage in while on Facebook were examined. Additional results will be analyzed as part of a larger study to gain further understanding of perceptions of white-collar crime. For example, participants were given the option to have their public Facebook profiles examined for types of personal information that could be used to answer categories of security questions. The participants who agreed will be contacted in the near future.

Procedure

A link to a Survey Monkey questionnaire was provided on the researcher's personal Facebook profile. This survey was only viewable to the researcher's Facebook friends. These friends were informed that they could voluntarily complete the study if they were over the age of 19. Facebook friends were also given permission to share the survey link through their own profiles. In an effort to recruit additional participants the link to the survey was also shared through the Grenfell Campus Messenger email, a daily email detailing ongoing events at Grenfell campus.

Participants who followed the link to Survey Monkey were first asked to read an informed consent notice. They were informed that the questionnaire assessed personal online experience and perceptions of online behaviour including the behaviour and experiences of an individual in a given scenario. Participants were asked to only click

"Next" if they were over the age of 19 and were voluntarily consenting to participate in the study. Participants were then able to begin the survey.

All participants completed the same survey questions in the same order with the exception of the third tier of the three-part scenario. Participants either read that the individual was being blackmailed or that the individual's email account was compromised. All questions were originally inputted with the intent that participants would randomly be sent to scenarios with differing endings. As a result of human error, of the 501 participants who were used in analysis, the first 256 received the blackmail scenario. The error in randomization was discovered after 2 weeks of data collection, and the questionnaire was modified appropriately so that future participants would therefore only receive the email compromised scenario. There was no indication made to participants that they would receive either scenario, nor that there was more than one scenario available to read. For the purpose of this study, only answers to the first part of this scenario, which all participants received, was analyzed. The questionnaire link was made available for a total duration of 1 month.

After completing the survey, participants were asked if they would be interested in having their Facebook profile examined by the researcher from a Facebook account created solely for the purpose of this study. They were informed that the researcher could assess the type of information made public on the participant's Facebook account and could compare that information to common security questions. Participants would then be asked to confirm only the number of questions which could be accurately answered with the information (e.g., favorite movie). A summary of information obtained from the participant's profile would be made available to him/her. If consent was given,

participants were provided with the researcher's e-mail to contact her directly. This information is not included in this thesis but rather will be collected as part of future research on the topic matter. All participants were provided with a debriefing notice after reaching the end of the survey.

Results

A series of descriptive and inferential statistics were used to interpret participants' understanding of the risk of exposure to white collar crime on the internet, participants' own negative online experiences, participants' ratings of white collar crimes relative to other online threats, and the behaviours participants reported engaging in during online activity that could potentially put themselves and others at risk. Gender differences were not examined there were large discrepancies between the number of men and women.

Recognition of Risk

To determine whether active Facebook users recognize their risk for exposure to white-collar crime in the details posted on their Facebook profiles, participants were provided with a list of 10 pieces of information commonly posted on Facebook profiles (e.g., pet's name, hometown, graduation class) that can either be used as answers or clues to answers for common security questions. Participants were asked to indicate what pieces of information from those listed could put someone at risk for deception for the purpose of financial gain and a number of other online threats. Figure 1 illustrates the proportion of participants indicating specific pieces of information that would put an individual at risk for deception for the purpose of financial gain. The other online threats surveyed will not be analyzed for the purposes of the current study.

Participants, upon completing the entire survey, were finally asked a question regarding their concern for white-collar crime. They were informed that the information commonly posted online (e.g., Hometown) can answer security questions. Four-hundred and thirteen participants rated their average concern from 1 (*Not concerned at all*) to 5 (*Very concerned*) to be 3.39 (SD = 1.15).

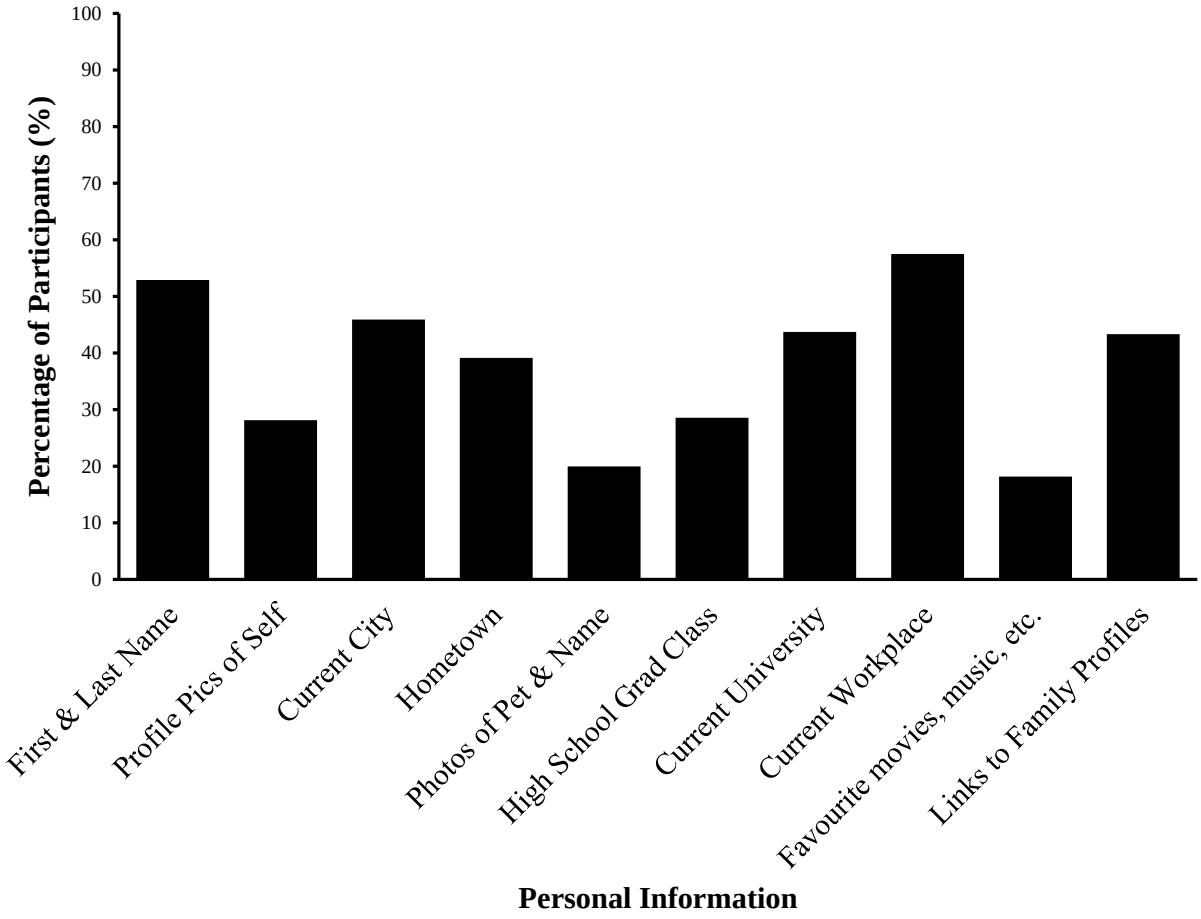

Figure 1. Percentage of respondents who identified risk for white-collar crime based on given information.

Experiences of Compromised Privacy

To assess whether online security breaches are common, participants were asked whether someone had ever logged into their Facebook account without the participant's knowledge or consent. Twenty-six percent of participants representing 129 individuals indicated that they had had an experience where someone signed into their Facebook profile without their knowledge or consent. As a more general measure of Facebook security, participants were asked whether they had ever had an experience where they felt their privacy was compromised on Facebook. A total of 184 respondents representing

37.1% of the sample indicated that yes they had. When participants were asked if they had ever had an experience where they felt that their privacy had been compromised on an online e-mail account, online bank account, or on the internet in general, 42.2% of individuals representing 208 respondents said yes.

Participants whose privacy was compromised online in general briefly described the experience. The majority of experiences (61.8%) described involved the participant losing control of an e-mail account ($N = 84$). However, 15 participants (11%) of those who elected to describe an experience, described one whereby an online baking account was compromised, or rather, the owner lost control. A further breakdown of responses can be seen in Figure 2.

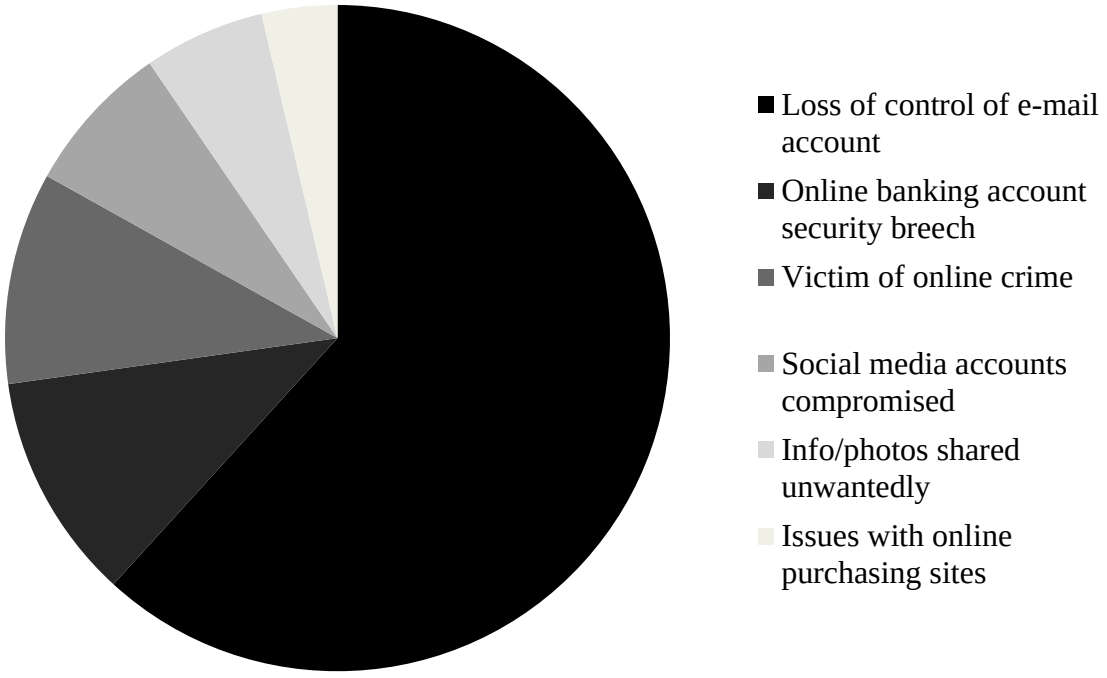

Figure 2. Participant experiences whereby privacy was compromised online.

Ranking of Threats

To determine whether white-collar crime was perceived as less serious than other risky online activities, participants were asked to rank six online behaviours from 1 (*Most serious*) to 6 (*Least serious*). Unfortunately, a number of participants misunderstood the question and did not differentiate between the six online behaviours but rather ranked the severity of each behaviour on a scale of 1 to 6. For example, participants identified two behaviours as being the most serious by ranking them both as 1 (*Most serious*). Those who misunderstood the question were excluded from the analysis leaving a total of 340 participants. Descriptive statistics, including means and standard deviations of participant responses, can be seen in Table 1.

Table 1

Average Ranking of Perceived Seriousness of Online Threats

Online threat	*M*	*SD*	*n*
Identity theft	2.08	1.52	340
Bullying/harassment	2.77	1.48	340
White-collar crime	3.30	1.20	340
Tracking	3.42	1.29	340
Third party usage	4.22	1.24	340
Gossip	5.16	1.59	340

A repeated measures ANOVA was used to analyze where participants ranked the behaviours in terms of severity. Mauchley's test of sphericity was violated and for that reason, Greenhouse Geiser was used to correct the violation. The ANOVA indicated significant differences between the participants' ratings of the six online behaviours, $F(3.66, 1241.46) = 171.13$, $p < .001$, partial $\eta^2 = .34$. Post-hoc tests indicated that there was a significant difference between deception for the purpose of financial gain (white-collar crime) and identity theft (mean difference = 0.53, $p < .001$). The ranking for white-collar crime was also significantly different than bullying/harassment (mean difference = 1.221, $p < .001$), third party usage (mean difference = -0.92, $p = < .001$), and gossip (mean difference = -1.85, $p < .001$). There was no significant difference found in ranking the severity of deception for the purpose of financial gain and the severity of personal information being used to track someone's whereabouts (mean difference = -0.12, $p = .291$).

Behaviours

To determine whether participants were engaging in behaviours that put themselves and others at risk, participants were asked a series of questions pertaining to their personal accounts, online behaviours and understanding of Facebook policies. When asked to rate the overall privacy of their Facebook accounts on a scale from 1 (*Not private at all*) to 5 (*Completely private*) on average, participants rated the overall privacy of their accounts to be 3.04 ($SD = 1.04$, $n = 500$). Only 25 respondents (5%) indicated that their accounts were fully private. When asked about their practice of accepting Facebook friends, 47% of respondents, representing 233 participants, indicated that they had accepted a Facebook friend whom they did not know prior to Facebook contact.

Using Facebook without a full awareness or understanding of Facebook's policies could be considered a risky online behaviour to the self. Therefore, participants were asked questions regarding their awareness of Facebook's Data Use Policy. Of 497 respondents, 61% were unaware that Facebook has a Data Use Policy. Of the 39% who were aware of the Data Use Policy, 91.2% had not fully read the policy (n = 194). In order to assess the level at which those who had fully read the Data Use Policy felt they understood the policy, those who had fully read it were asked to rate their level of understanding of the complete policy. Respondents indicated that on a scale from 1 (*Do not understand*) to 5 (*Completely understand*), on average, their level of understanding was 3.21 (SD = 1.03, n = 19). Out of the 19 participants who had fully read it, only 2 respondents indicated they completely understood the Data Use Policy.

Of 497 respondents, 53.3% were unaware that Facebook has a Statement of Rights and Responsibilities (SRR). Of the 46.7% who were aware of the SRR (265), 94% of them indicated they had not fully read the Statement of Rights and Responsibilities (n = 263). Out of the 15 participants who had fully read the SRR, the average understanding as rated from 1 (*Do not understand*) to 5 (*Completely understand*) was 3.13 (SD = 0.83). No one indicated that they fully understood the SRR (n = 15).

When Facebook users were asked about their viewing practices as they pertain to the public profiles of others, 97% of respondents (n = 491) indicated they had viewed someone's public Facebook profile to determine information about that individual. Participants who did not deny viewing someone's profile to gain information were asked to indicate on a scale of 1 (*Never*) to 5 (*Almost always*) how often they used Facebook

profiles to find information about someone else. Among participants, the average frequency of relying on Facebook profiles for information was 3.61 (*SD* = 1.10, *n* = 470).

Discussion

Given that white-collar crime is an existing threat online, there are a multitude of questions regarding online security. The present study, through the assessment of perceptions of online white-collar crime and online behavior, provides important answers. Overall, it can be deduced that active Facebook users are not recognizing the risk for white-collar crime in the information commonly disclosed online. Furthermore, active Facebook users are potentially disclosing personal information via Facebook that can be used to answer online security questions. Despite the continuous risk for white-collar crime, current perceptions do not match reality.

Recognition of Risk for White-Collar Crime

The results of the study suggest that active Facebook users do not recognize the risk for white-collar crime associated with posting personal information online, thus supporting the first hypothesis. Participants were provided with a list of personal details commonly posted on Facebook (e.g., High School graduation class) and were asked to indicate which of these could put someone at risk for white-collar crime. The results overwhelmingly indicated that participants do not recognize that such information can be used to answer security questions.

The information flagged by the most participants as being risks for white-collar crime were providing first and last name, as well as current workplace. However, just over one half of participants recognized providing these as being risky behaviour. Furthermore, less than 20% of participants recognized how posting a pet name and personal interests could be unsafe. As previously explained, the ways in which security questions can be categorized (e.g., family related, location related, animal related,

personal interest related) corresponds with how information posted on Facebook can be organized. The information that participants did not flag as unsafe to post can be used to answer corresponding questions such as "What is the name of your first pet?" or "What is your favourite band?" These are common security questions (Just, 2004; Rabkin, 2008). For example, a Yahoo e-mail account could be secured with one of two security questions related to the user's taste in music. Considering that all of the information listed to respondents can answer, or provide clues to the answers for security questions, the percentages of participants recognizing that provision of such information is risky are considerably low.

Reality versus Perception

An experience whereby personal information on Facebook is not in the control of the owner means that another individual may have an answer to an online security question. It is a substantial concern that 184 of 469 participants (37%) indicated they had an experience on Facebook where they felt that their privacy was compromised. This demonstrates that there are privacy risks when using Facebook. Furthermore, 208 of 493 individuals (42%) had an experience whereby they felt that their privacy was compromised online, outside of Facebook. Of those who described their experience, the majority of incidents whereby privacy was violated involved e-mail accounts (n = 84) and online banking (n = 15). This demonstrates a prevailing possibility for white-collar crime because personal information such as pay cheques and bank statements can arrive via personal e-mail addresses. The second hypothesis was thus supported.

Despite evidence suggesting personal information is frequently jeopardized, participants ranked white-collar crime below two other online behaviours out of six.

Considering that white-collar crime is not seen as a serious crime compared to other offenses, it is not surprising that such perceptions have been carried into the online community (Holtfreter et al., 2008; Rosenmerkel, 2001; Rossi et al., 1974). Participants ranked deception for the purpose of financial gain third in seriousness under identity theft and bullying/harassment, but above tracking, third party usage and gossip. Therefore, the third hypothesis that white-collar crime would be rated as less serious than other online threats was partially supported. Notably, it is a positive sign that identity theft was ranked as the most serious online behaviour. Identity theft can be used as a step towards white-collar crime. For example, a perpetrator may assume another's identity to deceive others for financial gain or he/she could take out a bank account in the victim's name. Furthermore, it is possible that bullying/harassment was seen as more serious than white-collar crime due to its frequent appearance in the media. Considering that only 16 of 240 respondents ranked white-collar crime as the most serious issue, it is possible that lack of current attention is responsible. While all the behaviours provided to participants are important and each has its own negative consequences, it is hopeful that future education will highlight white-collar crime as being dangerous both personally and financially (Abel, 2008).

Implications of Risky Online Behaviours

The results of the current study indicate that active Facebook users are engaging in behaviours that leave personal information open to white-collar criminals, supporting the fourth hypothesis. It is this personal information that can be used to answer important security questions. A number of examples of risky conduct emerged in the results of the survey. For example, participants perceived their profile privacy to be lower than ideal,

which could mean that personal information is exposed. In the survey, privacy was defined as the degree to which anybody other than Facebook friends could access profile information. Participants indicated that on average, they believed their Facebook profile privacy was a 3.04 on a scale from 1 (*Not private at all*) to 5 (*Completely private*). This suggests that Facebook users are not taking advantage of the maximum level of privacy available on their Facebook accounts. However, it may take a perceived personal risk or a negative experience before participants increase their security settings (Christofides et al., 2012; Debatin et al., 2009). Regardless, there are simple steps to help increase privacy and reduce the chance of white-collar crime being committed through the stealing of personal information. With maximum privacy settings, users can only show their name as indicated, and a profile photo of one's choosing to a non-Facebook friend. Accounts can also be made non-searchable. The ideal rating of privacy, indicative of maximized protection against online crime, would be 5/5.

Another result supporting the hypothesis that active Facebook users are engaging in risky behaviours is the high number of participants who accepted strangers as Facebook friends. A Facebook profile that offers information to the public (e.g., non-Facebook friends) is not the only way to put the profile owner in danger. For example, a pet's name shown only on a private Facebook page is no longer protected when a stranger's friend request is accepted. Of 496 respondents, 233 indicated that they had accepted someone as a Facebook friend whom they did know prior to Facebook to contact. This suggests that nearly half (47%) of active Facebook users are allowing strangers to view their personal and complete profile. Findings correspond with the outcomes of Sophos' (2009) study, who demonstrated that 43.5% of contacted Facebook

users accepted an artificial Facebook user as a friend. Accepting other Facebook users without a personal connection is common practice (Lemieux, 2012; Sophos, 2009). This is exposing personal information to strangers who may then use that information in criminal activity. A pet name can be used to answer or provide a clue to answer the security question, "What is the name of your favourite pet?" Accepting strangers as Facebook friends exposes the entirety of posted information. This also creates risk for other dangers such as stalking and unwanted contact.

Facebook users are also engaging in behaviours that take advantage of personal information being readily available online. When asked if they had ever examined a public Facebook profile to obtain information about the owner of the account, an overwhelming majority of participants (97%) indicated that they had. Because almost all respondents claimed that they have used Facebook to find information about another person, this suggests Facebook is a source for obtaining information about others. However, Chalk and Jones (2011) found that over half of Facebook users denied that their accounts were used to determine information about them by acquaintances. This indicates a reality far different than perception. White-collar criminals can begin the process by using the profiles of others to obtain information. The behaviours, as indicated to occur by respondents in the current study, show that Facebook users frequently begin this process.

Facebook offers ways in which users may adjust the privacy settings on their personal profiles. Information on how to change privacy settings, and also the limitations of privacy on Facebook, are available in the Data Use Policy and Statement of Rights and Responsibilities. The Data Use Policy is an essential document to understanding how

personal information posted on Facebook is used. However, 61% of active Facebook users surveyed were unaware that the policy even existed. This suggests that there may be some reason why the Data Use Policy is not a well-recognized document. It is possible that users simply skim through the information, later forgetting it exists. Of the 194 participants who were aware of the Data Use Policy, only 17 (8.8%) respondents had fully read the document. Of those 17, only two indicated that they fully understood it. Considering its importance, there may be a common reason why so few respondents had fully read the Data Use Policy. As it is a lengthy read, perhaps it is intimidating and difficult to understand. For example, the Data Use Policy consists of 9000 words and extends over seven pages when printed from the webpage. While Facebook has made changes to improve the layout of the Data Use Policy, the content remains the same. Thus far, conclusions regarding the Data Use Policy are based on personal investigation by the researcher. Further research would be of benefit.

Similarly, nearly half of participants were unaware of the Statement of Rights and Responsibilities (SRR). This is worrisome as the SRR must be read, acknowledged and accepted before anyone can use Facebook. Almost all who were aware of the SRR indicated that they had not fully read the document (94%). Like the Data Use Policy, at first glance the SRR appears to be a daunting read in terms of length, language and presentation style. For example, the SRR is nearly 4500 words and is six pages long. In the opinion of the researcher, it presents as a legal document with overly intricate wording for the layperson. Consider the following statement from the SRR, “you grant us non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License)” (Statement of

Rights and Responsibilities, 2013). Long sentences, undefined terms and small font may pose a problem. No participant in the current study indicated that they fully understood the policy. It must be considered however, that only the few who had fully read the SRR were asked to indicate understanding. Notably, users who did not fully read the SRR were not prompted to investigate the Data Use Policy, as the SRR encourages Facebook users to read and maintain knowledge of its policies.

Limitations and Future Research

There were potential limitations to the current study which must be taken into consideration. First, the methods by which the surveys were distributed may have limited the generalizability of the results to a larger and more diverse population. The survey link was made available on Facebook and through an e-mail newsletter specific to the Grenfell Campus. The link for the survey was posted on the researcher's personal page and viewable to her Facebook friends. Furthermore, because the survey was shared over Grenfell Messenger, only students and staff of Grenfell Campus were recruited outside of Facebook.

Second, this survey relied heavily upon participant memory. By questioning participant memory of privacy settings, online experiences, and Facebook policies, there was a potential for absent or inaccurate responses. For example, participants may have indeed read and accepted Facebook's Statement of Rights and Responsibilities, but forgotten this when completing the current survey.

Considering the results of the present study, there is opportunity for future research. Future research into white-collar crime could benefit from assessing youth under the age of 19 in their perceptions of white-collar crime and the risks of posting

personal information. Assessing a younger sample would fill a gap in the literature regarding the online habits of the younger generations who have grown up using the internet as a common tool. For example, Facebook will currently not allow anyone under the age of 13 to use the website. However, this leaves a number of unanswered questions. Can 13-year-olds recognize the risk for white-collar crime in posting their personal information? Are their perceptions for threat higher or lower than an older sample? If Facebook use can begin at age 13, there is a chance to examine perceptions that, with age, may influence the privacy of online accounts (e.g., online baking, online purchasing, emails).

Second, the current project assessed the recognition of white-collar crime online. Future research could assess the impact of education in online security. For example, education could include outlining the specific ways in which the personal details put on the internet (e.g., hometown) could be used to answer common security questions (e.g., where did you have your first kiss?). Questions which could be pursued include: Does education make a difference in perceptions of white-collar crime online? Does education lead Facebook users to increase privacy settings?

Third, the substantial unawareness regarding Facebook's Data Use Policy and Statement of Rights and Responsibilities (SRR) suggests that the next step in research should look closer at problems within Facebook which may contribute to the prevalence of white-collar crime. Some practical questions to ask would be: Is there a reason awareness in this sample was so low? Is there a reason some users are not fully reading nor understanding the policies Facebook implements? Are there features Facebook users would like to see implemented to better protect their personal information? By obtaining

a better understanding of problems within Facebook that may lead someone to skip potentially useful information (e.g., limitations to privacy of personal information, privacy control options), we may be able to understand how Facebook can take measures to better protect its consumers.

Conclusion

White-collar crime is a present-day concern for Facebook users, whether they recognize it or not. White-collar crime, manifesting in the abuse of trust and power for money, exists all around us. For example, in the recent case of missing student Loretta Saunders, there was an attempt at white-collar crime through Loretta's cell phone. The perpetrator in the case impersonated Loretta via text message, and asked Loretta's boyfriend to remind Loretta of her mother's maiden name ("Loretta Saunders's boyfriend: 'She meant everything to me," 2014). This example is meaningful as a mother's maiden name is a common security question for online banking. Correctly answering security questions opens up a world of financial gain to perpetrators who can successfully do so. Previous research, pranks, crimes and news reports have all demonstrated that security questions, such as a mother's maiden name, can be easily answered by the copious amounts of personal information available online (Christofides et al., 2009; Lemieux, 2012; Rabkin, 2008; Sophos, 2009). Results of the current study correspond with previous research in that Facebook users are engaging in behaviours that expose their personal information, and they do not recognize the risk for white-collar crime in doing so. With further research and education into online security, the safety of Facebook users will expectantly improve over time. Facebook users have the right to be informed so as

to best protect their personal information, and with that, the integrity of their online security questions.

References

Alexander, M. (2011). *Facebook and cyber monitoring: An exploratory study* (unpublished honours thesis). Grenfell Campus, Memorial University of Newfoundland, Corner Brook, Newfoundland.

Abel, C. F. (1985). Corporate crime and restitution. *Journal of Offender Counselling, Services & Rehabilitation, 9,* 71-94. doi:10.1300/J264v09n03_07

Candy Crush Saga. (n.d.). Retrieved from https://developers.facebook.com/docs/showcase/candycrushsaga/

Candy Crush Saga All Help. (n.d.). *Timeline* [Facebook page]. Retrieved April 16th, 2014, from https://www.facebook.com/groups/308519635921675/

Chaulk, K., & Jones, T. (2011). Online obsessive relational intrusion: Further concerns about Facebook. *Journal of Family Violence, 26,* 245-254. doi: 10.1007/s10896-011-9360-x

Christofides, E., Muise, A., & Desmarais, S. (2009). Information disclosure and control on Facebook: Are they two sides of the same coin or two different processes? *Cyberpsychology, Behavior, and Social Networking, 12,* 341-345. doi:10.1089/cpb.2008.0226

Christofides, E., Muise, A., & Desmarais, S. (2012). Risky disclosures on Facebook: The effect of having a bad experience on online behaviour. *Journal of Adolescent Research, 27,* 714-731. doi:10.1177/0743558411432635

Corporate Crime. (2012). Retrieved from http://www.rcmp-grc.gc.ca/ccb-sddc/index-eng.htm

Data Use Policy. (2013). *Facebook*. Retrieved from https://www.facebook.com/full_data_use_policy

Debatin, B., Lovejoy, J. P., Horn, A., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication, 15*, 83-108. doi:10.1111/j.1083-6101.2009.01494.x

Fraud costs Canadians $10B annually: RNC. (2010, June 1). Retrieved from http://www.cbc.ca/news/fraud-costs-canadians-10b-annually-rcmp-1.899733

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior, 25*, 153-160. doi:10.1016/j.chb.2008.08.006

Guillaume, D. (2012, September 4). Amazing mind reader reveals his 'gift'. Retrieved from http://www.youtube.com/watch?v=F7pYHN9iC9I#t=133

Helmkamp, J., Ball, R., & Townsend, K. (Eds). (1996). *Definitional dilemma: Can and should there be a universal definition of white collar crime?* Morgantown, WV: National White-Collar Crime Center.

Holtfreter, K., Van Slyke, S., Bratton, J., & Gertz, M. (2008). Public perceptions of white-collar crime and punishment. *Journal of Criminal Justice, 36*, 50-60. doi:10.1016/j.jcrimjus.2007.12.006

Houghton, D. J., & Joinson, A. N. (2010). Privacy, social network sites, and social relations. *Journal of Technology in Human Services, 28*, 74-94. doi:10.1080/15228831003770775

Just, M. (2004). Designing and evaluating challenge-question systems. *IEEE Security & Privacy, 2*, 32-39.

Lemieux, R. (2012). Fictional privacy among Facebook users. *Psychological Reports, 111*, 289-292. doi:10.2466/21.01.PR0.111.4.289-292

Loretta Saunders's boyfriend: 'She meant everything to me'. (2014, February 21). Retrieved from http://www.cbc.ca/news/canada/nova-scotia/loretta-saunders-s-boyfriend-she-meant-everything-to-me-1.2545968

Nosko, A., Wood, E., Kenney, M., Archer, K., De Pasquale, D., Molema, S., & Zivcakova, L. (2012). Examining priming and gender as a means to reduce risk in a social networking context: Can stories change disclosure and privacy setting use when personal profiles are constructed? *Computers in Human Behavior, 28,* 2067-2074. doi:10.1016/j.chb.2012.06.010

Praveen (2012, January 1). *How to: How to hack Facebook accounts, the traditional way*. Retrieved from http://www.techgadgetsweb.com/6622/to-hack-facebook-accounts-traditional/comment-page-1

Ramachandran, S. (2013, December). House robbed while neighbor watches, woman holds Facebook guilty. *Device Magazine*. Retrieved from http://www.devicemag.com/

Rabkin, A. (2008, July). Personal knowledge questions for fallback authentication: Security questions in the era of Facebook. Presentation at the Symposium on Usable Privacy and Security (SOUPS), Pittsburgh, PA. doi: 10.1145/1408664.140866 7

Rosen, R. J. (2012, August 7). Security questions: The biggest joke in online identity verification. *The Atlantic*. Retrieved from http://www.theatlantic.com

Rosenmerkel, S. P. (2001). Wrongfulness and harmfulness as components of seriousness of white-collar offenses. *Journal of Contemporary Criminal Justice, 17*, 308-327. doi:10.1177/1043986201017004002

Rossi, P. H., Waite, E., Bose, C. E., Berk, R. E. (1974). The seriousness of crimes: Normative structure and individual differences. *American Sociological Review, 39*, 224-237. doi:10.2307/2094234

Scoville, G. (2010, July 2). *Designing good security questions*. Retrieved from http://goodsecurityquestions.com/designing.htm

Shapiro, S. P. (1990). Collaring the crime, not the criminal: Reconsidering the concept of white-collar crime. *American Sociological Review, 55*, 346-65. doi:10.2307/2095761

Simpson, S. S. (2013). White-collar crime: A review of recent developments and promising directions for future research. *Annual Review of Sociology, 39*, 309-331.

Stutzman, F., Capra, R., & Thompson, J. (2011). Factors mediating disclosure in social network sites. *Computers in Human Behavior, 27*, 590-598. doi:10.1016/j.chb.2010.10.017

Sutherland, E. H. (1940). White-collar criminality. *American Sociological Review, 5*, 1-12.

Sutherland, E. H. (1945). Is 'white-collar crime' crime? *American Sociological* Review, 10, 132-139. doi:10.2307/2085628.

The Associated Press. (2013). *Number of active users at Facebook over the years.* Retrieved from http://news.yahoo.com/number-active-users-facebook-over-230449748.html

White-Collar Crime. (n.d.). Retrieved from http://www.fbi.gov/about-us/investigate/white_collar

Appendix A

Survey of Online Behaviour (Informed consent)

The purpose of this informed consent statement is to ensure that you understand the nature of the present study and your involvement in it. This study is being conducted by Katherine Rose as part of the course requirements for Psychology 4951 and Psychology 4959. I am under the supervision of Dr. Kelly Warren. The results of this study will be used to write a thesis, as a requirement of the honours program at Grenfell Campus, Memorial University of Newfoundland. The results of this thesis may be published in the future. The purpose of the study is to examine perceptions of online behaviour.

The survey should take approximately 15-20 minutes to complete. You will be asked to answer questions based on your personal online experiences and perceptions of online behaviour. Lastly, you will be presented with a scenario about someone else's online behaviour and experiences. You will be asked to answer questions based on your perceptions of the scenario. There are no wrong or right answers; I am only interested in your opinion. There are no obvious risks or benefits involved with your participation. All responses will remain anonymous and confidential. Results will be analyzed as group data. Please do not give away any identifying information. Your participation in this study is completely voluntary and you are free to withdraw at any time. If you have any questions or concerns, please feel free to contact me at krose@grenfell.mun.ca or my supervisor, Dr. Kelly Warren, at kwarren@grenfell.mun.ca.

By clicking "Next", you are consenting to participate in the study

Appendix B

Survey of Online Behaviour

1. Are you an active Facebook user?

   Active Facebook: A user who logs into their Facebook account at least once every 30 days

   Yes _____ No _____

2. How private do you believe your personal Facebook account is?

   Private: the degree to which anybody <u>other than your Facebook friends</u> can access your profile information. The more private an account is, the harder it is for others to access your profile. information.

   1 2 3 4 5

   Not private at all Completely private

3. Are you aware that Facebook has a Data Use Policy?

   Yes _____ No _____

   a. (If answered YES to #3) Have you <u>fully</u> read the Facebook Data Use Policy?

      Yes _____ No _____

   b. (If answered YES to #3) How well do you understand the information in Facebook's Data Use Policy?

   1 2 3 4 5

   Do not understand Completely understand

4. Are you aware that Facebook has a Statement of Rights and Responsibilities (SRR)?

   Yes _____ No _____

   a. (If answered YES to #4) Have you fully read the Facebook Statements of Rights and Responsibilities (SRR)?

      Yes _____ No _____

   b. (If answered YES to #4) How well do you understand the information in the Statement of Rights and Responsibilities (SRR)?

1 2 3 4 5

Do not understand Completely understand

5. Have you ever accepted a Facebook Friend who you did not know prior to Facebook contact?

   Yes _____ No _____

6. Have you ever had someone log into your Facebook account without your knowledge or consent?

   Yes _____ No _____

7. Have you ever had an experience where you felt that your privacy had been compromised on Facebook?

   Yes _____ No _____

   a. (If answered YES to #7) Please briefly describe the experience: _____

      I would rather not discuss the experience ___

8. Have you ever had an experience where you felt that your privacy had been compromised on an online e-mail account, online bank account, or on the internet in general (outside of Facebook)?

   Yes _____ No _____

   a. (If answered YES to #8) Please briefly describe the experience:

      _____

      I would rather not discuss the experience ___

9. Have you ever viewed someone's public Facebook profile to determine information about that individual?

   Yes _____ No _____

   a. (If answered YES to #8) How often do you view public Facebook profiles when you want to know information about an individual?

1	2	3	4	5
Never				Almost always

10. With 1 representing the most serious and 6 representing the least serious, please order the following online behaviours from 1-6 according to how serious you feel they are. For example, if each of these were to happen, consider which you would find the most and least problematic.

___ Bullying/Harassment

___ Somebody's identity being stolen and used by someone else

___ Deception for the purpose of financial gain

___ Gossip

___ Personal information being used to regularly track someone's whereabouts and activities

___ Third party companies using someone's information

11. Jamie joined a Facebook group for players of Candy Crush Saga, a popular Facebook game. By joining the group, Jamie's profile will now be made accessible to other members of the group. The information that others can see/ can be seen on Jamie's profile includes: *First and Last name, Profile pic of self, Current city of residence, Hometown, Photos of pet and pet name, High school graduation class, Current University, Current workplace, Favourite music, movies, TV shows and books, Links to family profiles including Mother, Brother and Sister.*

11. Using check marks, indicate what information could lead Jamie to be at risk for the occurrences listed across the top?

	Risks					
Information	Bullying/ Harassment	Someone's identity being stolen and used by someone else	Deception for the purpose of financial gain	Gossip	Personal information being used to regularly track someone's where-abouts and activities	Third party companies using someone's information
First and Last name						
Profile pic of self						
Current city						
Hometown						
Photos of pet and pet name						
High school graduation class						
Current university						
Current workplace						
Favourite music, tv shows, movies & books						
Links to family profiles including mother, brother and sister						

A friend informs Jamie that he received a message from Jamie's Facebook profile. In the message, "Jamie" claimed to be stranded in a remote location and asked the friend to transfer money to Jamie's bank account via e-mail (e-transfer). Jamie denies writing the message and is unable to log into Facebook because the password for the account has been changed.

12. How concerned should Jamie be?

1	2	3	4	5
Not concerned at all				Very concerned

13. How likely do you believe it is that Jamie's friend would send the money?

1	2	3	4	5
Not likely				Very likely

14. Which, if any of the following people do you feel would send the money? Please check all that apply.

    ____ Romantic partner

    ____ Grandparents

    ____ Sibling

    ____ Friend

    ____ Parents

    ____ Other (please specify) _____

Ending #1: Jamie later receives an e-mail from an unnamed stranger. The stranger's e-mail says that he/she has revealing photographs that Jamie had exchanged in a private Facebook conversation with a Facebook friend. The stranger tells Jamie that he/she will release the photographs to Jamie's close friends and family unless Jamie pays money. Jamie does not want friends or family to see the photographs due to their nature.

15. How likely do you think it is that Jamie would send the money?

1	2	3	4	5
Not likely				Very likely

16. What do you suggest Jamie do in this situation?

_____

17. How responsible do you believe Jamie is for being in this dilemma?

1 2 3 4 5

Not at all responsible Completely responsible

18. What is the likelihood that the individual who has control over Jamie's Facebook account will be caught?

1 2 3 4 5

Not likely Very likely

Ending #2: The password to Jamie's e-mail account has also been changed, meaning that Jamie cannot access any e-mails. Without this access, Jamie worries about sensitive information being available to whomever has changed the password. Jamie's credit card statements, online purchases, student information and employee details all come through the same e-mail address.

19. What do you suggest Jamie do in this situation?

_____

20. How responsible do you believe Jamie is for being in this dilemma?

1 2 3 4 5

Not at all responsible Completely responsible

21. What is the likelihood that the individual who has control over Jamie's Facebook account will be caught?

1 2 3 4 5

Not likely Very likely

22. A recent examination of the public profiles of 200 Facebook users indicates that:

- 83% (166) provided a profile picture of themselves
- 52.5% (105) publicized their hometown
- 48% (96) revealed the names of family members (including fiancé, spouse and in-laws)
- 11.5% (23) gave the name of a pet
- 53.5% (107) provided details about their education (i.e. elementary school, high school graduation year, college degree etc.)

Information related to physical appearance, past locations, family members, pet names and education may be used to answer important security questions for online accounts. This puts users at risk for white-collar crimes such as fraud, Ponzi schemes and/or identity theft. Based on this information, how concerned are you that the details made public on your account may put you at risk?

1	2	3	4	5
Not concerned at all				Very concerned

Age: _____

Gender: _____

Would you consent to having your profile assessed from a separate Facebook account to see what type of information is made available to the public?

With your consent, your Facebook profile will be viewed from a Facebook account created solely and temporarily for the purpose of this study. After your profile has been studied, you will be provided with a summary of the information made available to the public on your profile. You will be asked to confirm the number of questions I can accurately answer with the information and you will be asked to answer some post-survey questions. Only your indication of the number of details I have accurately obtained in various categories (i.e favourite movie) will be used in the study. No personal information (i.e. the name of your favourite movie) will be collected or used. Your profile will remain anonymous and results will be analyzed using group, not individual, data.

Please indicate with a checkmark (✓)

Yes, I give consent to have the nature (i.e. favourite movie) and accuracy (i.e. number of details) of information collected from my public profile used in the study. _____

Appendix C

Survey of Online Behaviour (Debriefing screen)

The purpose of this study is to examine perceptions of white-collar crime on the internet. White-collar crime occurs when those in positions of power use deception to make money. The information made available on Facebook profiles may put users at risk for white-collar crime. I want to study whether white-collar crime is perceived to be a serious online threat. Furthermore, I am interested in whether members of Facebook can recognize the risk for white-collar crime in a scenario where particular information is made available on a Facebook profile. I am also interested in public perceptions of online white-collar crime, including victim responsibility, risk to the individual's security and the recommended course of action. I ask that until all results have been collected and analyzed that you do not discuss the specific nature of the study with others.

All data collected is anonymous and will be kept confidential. Results will be analyzed as group data, not as individual data. If you have any questions or concerns about the study, feel free to contact myself at krose@grenfell.mun.ca or my supervisor, Dr. Kelly Warren, kwarren@grenfell.mun.ca. If you are interested in knowing the results of the study, you may contact myself or Dr. Kelly Warren any time after April 22nd, 2013. If this study raised any personal concerns for you, please contact a counsellor at Kids Help Phone via telephone 1-800-668-6868 or online at www.kidshelpphone.ca. You may also find more information about online safety at www.respect-yourself.ca or http://www.rcmp-grc.gc.ca/is-si. Thank you for your time and cooperation in completing the survey.